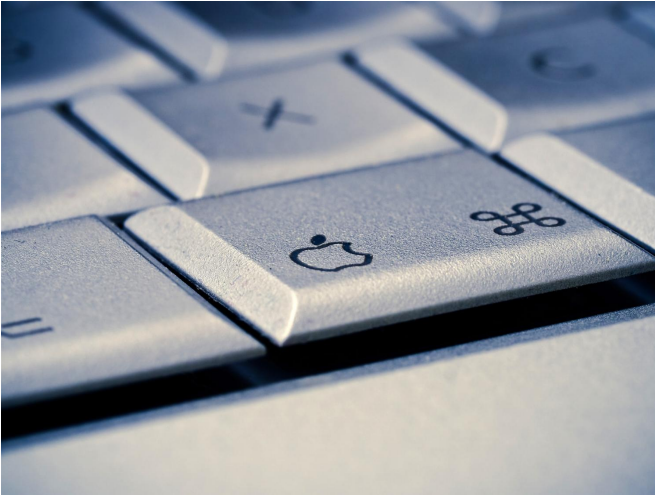


Hackers locking Mac machines demand ransom

26 September 2017, by Nancy Owano



Credit: CC0 Public Domain

(Tech Xplore)—Find My device is a service indeed—not only to Apple device owners but, guess who, to hackers.

At least in the sense that reports have been surfacing posted by hapless users of being locked out of their screens and told to pay up in Bitcoin.

It's easy to lock a Mac with a passcode in Find My iPhone if you have someone's Apple ID and password, said *MacRumors*.

Christina Bonnington in *The Daily Dot* also said hackers could use the Find My feature to lock your [device](#) remotely and hold it for ransom.

She said these hackers are finding the Find My iPhone and desktop counterpart Find My Mac useful.

"If they learn your Apple ID and password, they can use it to remotely lock your device and hold it for [ransom](#)."

The device lock is accompanied by the message on your screen, asking you to pay up.

Lifehacker writer Nick Douglas reported that a Twitter user talked about a ransom note on a hacked Mac. "The [hacker](#) asks for Bitcoin, the ransom currency of choice, as it's hard to trace," Douglas said.

Jon Martindale in *Digital Trends*: The ransom message is delivered on the lock screen itself, often with a Bitcoin wallet address. In the case of one user, their hacker demanded 0.01 Bitcoin to unlock the device, or around \$40.

Paying up, though, "only emboldens hackers to continue the practice," Martindale remarked. "The best bet would be to contact Apple directly to help solve the problem."

More advice? Good luck with that. A number of sites had their own suggestions but few were in unison except for two consistent threads: (1) Update your ID passwords. (2) Don't pay the clowns.

Tyler Lee in *Ubergizmo*: "In order to prevent yourself from being hacked, users are recommended to update their Apple [ID](#) passwords as well as enable [two-factor authentication](#). Those who have been affected are also recommended to get in touch with Apple to have their computers unlocked."

Lifehacker recommended in an update that "We stand by our advice to turn off "Find My Mac." ... "Find My Device" still poses a potential back door for remote attacks on any Mac, and on any iPhone without a passcode. Still, many readers will prefer the risk of remote attacks to the risk of never [recovering](#) a stolen device."

Also, using the same password in multiple places is not a good idea, considering these scenarios.

Juli Clover, an editor at *MacRumors*: "Apple users should change their Apple ID [passwords](#), enable two-factor authentication, and never use the same password twice."

Digital Trends said, "it would behoove you to use strong passwords, unique login credentials and two-factor [authentication](#) where possible."

Interestingly, a reader comment from someone who has done "computer security for a living," said that your phone was much more likely to be physically stolen than to be exploited in this manner.

Any incidents of such a thing in the real world? Yes. How did hackers get these people's passwords? Clover said the usernames and passwords of the iCloud accounts affected were likely found through various site data breaches and not through a breach of Apple's servers.

The hackers will need access to your iCloud username and password, said *Ubergizmo*. Once they have that, they can remotely lock a Mac computer using the passcode.

Moreover, said Clover, "Impacted users likely used the same email addresses, account names, and passwords for multiple accounts, allowing people with malicious intent to figure out their iCloud details."

BGR: "As long as you don't reuse [passwords](#), and your iCloud login is distinct from any of your [username](#) and password combo that may have been affected by a recent hack, you are safe," said Chris Smith.

© 2017 Tech Xplore

APA citation: Hackers locking Mac machines demand ransom (2017, September 26) retrieved 20 October 2019 from <https://techxplore.com/news/2017-09-hackers-mac-machines-demand-ransom.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.